PREGLED POSTUPKA #104706

1 PODACI O NARUČIOCU

Naziv naručioca	AGENCIJA ZA SPREČAVANJE KORUPCIJE
PIB	11006507
E-mail	kabinet@antikorupcija.me
Telefon	020/447-702, 202/447-723
Internet adresa	www.antikorupcija.me
Fax	020/234-082
Adresa	Ulica Kralja Nikole 27/V
Grad	Podgorica
Poštanski broj	81000

2 OSNOVNI PODACI

Opis predmeta javne nabavke	DLP and Clasification softver
Status	U toku
Vrsta predmeta	Usluge
Vrsta postupka	Jednostavna nabavka
Službenik za javne nabavke	Dragana Dacić
Kontakt	020-447-718
Datum objave	04.12.2025. 12:50
Napomena	-

3 FAZE U POSTUPKU

Vrsta faze	Opis	Početak podnošenja	Kraj podnošenja	Datum otvaranja	Status
Zahtjev za podnošenje ponuda	Zahtjev za podnošenje ponuda - DLP and Clasification softver	04.12.2025 12:50	08.12.2025 10:00	08.12.2025 10:00	U toku

4 DODATNE INFORMACIJE

Predmet javne nabavke se nabavlja	kao cjelina
Posebni oblici javne nabavke	
Okvirni sporazum	Ne
Dinamički sistem nabavki	Ne
Elektronska aukcija	Ne
Elektronski katalog	Ne
Nabavka se sprovodi kao	
Zajednička nabavka	Ne
Centralizovana nabavka	Ne
Nabavka je	
Zelena	Ne
Društveno odgovorna	Ne

5 STAVKE PLANA

Godina	Opis	Vrijednost nabavke	Vrijednost PDV	Okvirni sporazum	Vrijednost OS	Vrijednost PDV OS	Vrsta postupka
2025	**AGENCIJA ZA SPREČAVANJE KORUPCIJE** **DLP and Clasification softver** 48731000 - Softverski paket za bezbjednost fajlova	13.000,00 EUR	2.730,00 EUR	-	-	-	Jednostavna nabavka

6 USLOVI ZA UČEŠĆE U POSTUPKU I ZAHTJEVI U POGLEDU NAČINA IZVRŠAVANJA PREDMETA NABAVKE

Opis	Tip uslova / zahtjeva
Uz ponudu se dostavlja Izjava ponuđača o ispunjenosti uslova utvrđenih zahtjevom i nepostojanju sukoba interesa, potpisana od strane ovlašćenog lica ponuđača, data na Obrascu 2, preuzimanjem na posebnom aplikativnom dijelu elektronskog sistema javnih nabavki, shodno članu 9 stav 10 Pravilnika o načinu sprovođenja jednostavnih nabavki („Službeni list CG“, br. 16/23, 20/23, 36/23, 114/23, 49/24 i 114/24)	Obrazac 2
Mjesto izvršenja ugovora je sjedište Agencije za sprečavanje korupcije, Ulica Kralja Nikole 27/V, Podgorica	Mjesto izvršenja ugovora
Rok važenja ponude: 60 dana od dana otvaranja ponuda	Rok važenja ponude
Način plaćanja: virmanski, na žiro račun Izvršioca. Žiro račun:_____ Banka:_____ (Ponuđač je obavezan navesti broj žiro računa i banke).	Način plaćanja
Ponuđač je dužan da obezbijedi: • tehničku dokumentaciju (instalacija, konfiguracija, administracija) • korisnička uputstva (za administratore i po mogućnosti za krajnje korisnike) • preporuke za najbolje prakse u primjeni DLP i klasifikacije u organizaciji	Drugi uslovi
Rok za isporuku sistema ne smije biti duži od 10 dana od dana potpisivanja ugovora	Rok izvršenja ugovora
Sprovođenje kontrole kvaliteta vršiće službenici Odsjeka za informacione tehnologije Agencije.	Način sprovođenja kontrole kvaliteta
Plaćanje će se vršiti u roku do 30 dana nakon dostavljanja fakture i potpisivanja zapisnika o izvršenoj usluzi koji će potpisati predstavnici naručioca i izvršioca. Uredno ispostavljena faktura i zapisnik o izvršenoj usluzi potpisan od strane predstavnika Naručioca i Izvršioca predstavlja osnov za plaćanje ugovorene cijene	Rok plaćanja

Izabrani ponuđač je dužan da obezbijedi: -tehničku dokumentaciju (instalacija, konfiguracija,administracija) -korisnička upustva (za administratore i po mogućnosti za krajnje korisnike) -preporuke za najbolje prakse u primjeni DLP i klasifikacije u organizaciji	Drugi uslovi

7 KRITERIJUMI ZA IZBOR NAJPOVOLJNIJE PONUDE

Opis
Cijena

8 PREDMET NABAVKE

Procijenjena vrijednost nabavke: **13.000,00 EUR**

TEHNIČKA SPECIFIKACIJA PREDMETA NABAVKE

	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina
		1. Predmet nabavke Predmet ove nabavke je isporuka, implementacija i održavanje softverskog rješenja za: • Data Loss Prevention (DLP) – sprječavanje neovlašćenog iznošenja i curenja podataka • Data Classification – klasifikaciju i označavanje podataka prema nivou osjetljivosti Rješenje treba da obuhvati min. 70 radnih stanica i 10 servera, sa centralizovanim upravljanjem i izvještavanjem. 2. Okruženje i obim 2.1. Mrežno okruženje • Zatvorena ili kontrolisana korporativna mreža • Direktorijumska infrastruktura zasnovana na Active Directory ili ekvivalentu • Pristup internetu ograničen kontrolisan preko firewall 2.2. Klijentske radne stanice • Min. 70 radnih stanica • Operativni sistemi: o Microsoft Windows 10 / 11 (64-bit) o Poželjno: podrška i za buduće verzije Windows OS tokom trajanja ugovora	

2.3. Serverska infrastruktura
• Min. 10 servera
• Operativni sistemi:
o Microsoft Windows Server 2016 ili noviji
• podrška za virtualizacione platforme (VMware, Hyper-V)
2.4. Centralne komponente
• Centralni server(i) za:
o upravljanje DLP i Classification politikama
o skladištenje logova i događaja
o generisanje izvještaja
• Mogućnost instalacije on-premise u okviru postojećeg data centra Naručioca na Vmware virtuelnoj mašini.

3. Funkcionalni zahtjevi – Data Loss Prevention (DLP)
DLP rješenje mora da obezbijedi najmanje sljedeće:
3.1. Zaštita na endpoint-ima (radne stanice i serveri)
• Praćenje i kontrola:
o kopiranja fajlova na USB uređaje i druge izmjenjive medije
o printanja dokumenata sa osjetljivim podacima
o slanja fajlova preko e-mail klijenta (npr. Outlook)
o upload-a fajlova na web i cloud servise (HTTP/HTTPS)
o kopiranja u clipboard
o snimanja ekrana (screenshot / screen capture), gdje je podržano
• Mogućnost definisanja akcija po pravilu:
o dozvoli (allow)
o upozori (alert / warn)
o blokiraj (block)
o dozvoli uz obrazloženje ili override uz logovanje (justification / override)
3.2. Prepoznavanje osjetljivih podataka

		• Prepoznavanje osjetljivih podataka na osnovu: o unaprijed definisanih obrazaca (npr. brojevi ličnih dokumenata, brojevi kartica, sl.) o ključnih riječi, fraza, regularnih izraza o metapodataka i oznaka klasifikacije (vidi poglavlje 4) 3.3. Politike i pravila • Centralno definisanje i upravljanje DLP politikama • Mogućnost primjene politika: o po korisniku / korisničkoj grupi o po uređaju / grupi uređaja o po lokaciji podataka (lokalni disk, mrežni share, server, itd.) • Mogućnost definisanja posebnih politika za: o rad sa podacima unutar mreže o slanje podataka van mreže (internet, eksterni partneri) 3.4. Logovanje i izvještavanje • Detaljno logovanje svih DLP događaja (ko je, kada, sa kog uređaja, koji fajl, koja akcija) • Standardni i prilagodljivi izvještaji: o po korisniku o po tipu incidenta o po lokaciji podataka o po nivou ozbiljnosti • Izvoz izvještaja u najmanje jedan od sledećih formata: PDF, CSV, XLSX 3.5. Skalabilnost i performanse • Rješenje mora podržavati najmanje 55 endpoint-a (50 radnih stanica + 5 servera) • Ne smije značajno degradirati performanse na radnim stanicama (maks. prihvatljivo opterećenje CPU/memorije u skladu sa industrijskom praksom)	

1	Data Loss Prevention (DLP) – sprječavanje neovlašćenog iznošenja i curenja podataka i Data Classification – klasifikaciju i označavanje podataka prema nivou osjetljivosti	4. Funkcionalni zahtjevi – Data Classification 4.1. Model klasifikacije • Mogućnost definisanja najmanje 4 nivoa osjetljivosti (primjer, može da se prilagodi): o Public (Javno) o Internal (Interno) o Confidential (Povjerljivo) o Restricted / Highly Confidential (Strogo povjerljivo) 4.2. Označavanje podataka • Ručno označavanje klasifikacije od strane korisnika (npr. kroz integraciju u Office aplikacije ili kontekstni meni OS-a) • Automatska klasifikacija na osnovu: o sadržaja dokumenta (content inspection) o unaprijed definisanih šablona / pravila • Podržano označavanje: o dokumenata (npr. Office, PDF, tekstualni fajlovi) o e-mail poruka o po mogućnosti i drugih tipova fajlova (slike, arhive, itd.), gdje je primjenljivo 4.3. Vidljiva i nevidljiva obilježja • Mogućnost dodavanja: o vidljivih oznaka (header, footer, watermark) u dokument o nevidljivih oznaka / metapodataka (tagovi) za potrebe automatizovanog prepoznavanja • Integracija klasifikacionih oznaka sa DLP politikama (npr. dokument označen kao “Povjerljivo” ne smije se slati van organizacije). 5. Integracije Ponuđač mora opisati i obezbijediti sljedeće integracije: • Integracija sa Active Directory ili ekvivalentom radi:	1,00 paket

		o autentikacije korisnika o dodjeljivanja politika po grupama • Integracija sa Microsoft Exchange • Poželjno: API ili drugi mehanizam za integraciju sa postojećim SIEM / log management rješenjima (ako postoje). 6. Sigurnosni i tehnički zahtjevi • Komunikacija između agenata i centralnog servera mora biti šifrovana (TLS ili ekvivalent) • Centralna konzola mora imati: o role-based access control (RBAC) – različiti nivoi prava (administrator, auditor, helpdesk, sl.) • Sistem mora omogućiti: o backup i restore konfiguracije i politika o arhiviranje logova u skladu sa politikama Naručioca • Softver mora biti podržan od strane proizvođača tokom trajanja ugovora (security patch-evi, update-i) 7. Licenciranje Ponuđač je dužan da u ponudi jasno navede model licenciranja i uključi sve potrebne licence za: • Min. 50 radnih stanica (endpoint licenca) • Min. 5 servera (server licenca, gdje je primjenljivo) • licence za centralni server / konzolu i eventualne module potrebne za punu funkcionalnost (DLP + Classification) Prihvatljivi modeli licenciranja: • po endpoint-u (po uređaju) • po korisniku, uz uslov da je jasno navedeno koliko korisnika se pokriva i da obuhvata sve radne stanice i servere u obimu ove nabavke Ponuda mora da sadrži:	

		• trajanje licence: o trajne licence sa obaveznim ugovorom o održavanju (min. 3 godine), ili o subscription licence sa uključenim održavanjem i podrškom, min. 3 godine • jasno naznačene godišnje troškove: o licenci o održavanja i podrške 8. Implementacija, migracija i obuka Ponuda treba da uključi: 8.1. Implementacione usluge • Instalaciju centralnog servera / konzole • Instalaciju i konfiguraciju agenata na 50 radnih stanica i 5 servera • Definisanje početnog seta politika: o osnovne DLP politike o osnovni model klasifikacije (oznaka i pravila) • Testiranje funkcionalnosti u dogovoru sa Naručiocem 8.2. Obuka • Obuka za administratore (min. 1 dan): o upravljanje politikama o rad sa konzolom o pregled i analiza logova / incidenta • Kratka obuka / uputstvo za krajnje korisnike o kako da koriste klasifikacione oznake o šta se dešava kada DLP blokira neku akciju 8.3. Dokumentacija Izabrani ponuđač je dužan da obezbijedi: • tehničku dokumentaciju (instalacija, konfiguracija, administracija)	

		• korisnička uputstva (za administratore i po mogućnosti za krajnje korisnike) • preporuke za najbolje prakse u primjeni DLP i klasifikacije u organizaciji 9. Podrška i održavanje • Helpdesk podrška: o min. e-mail i telefonska podrška u radno vrijeme Naručioca • Vrijeme reakcije na prijavu problema: o kritične greške – maksimalno vrijeme reakcije 4h o ostale greške –8h / sljedeći radni dan • U okviru održavanja mora biti obuhvaćeno: o pravo na sve sigurnosne zakrpe i verziona unapređenja tokom trajanja ugovora o pomoć u rješavanju incidenata vezanih za DLP/Classification sistem 10. Kriterijumi usklađenosti ponude Ponuđač mora u ponudi jasno naznačiti: 1. Da li ponuđeno rješenje ispunjava svaki od gore navedenih zahtjeva (DA/NE uz eventualno pojašnjenje). 2. Model licenciranja i ukupni broj uključenih licenci. 3. Usluge implementacije i obuke koje su uključene u cijenu. 4. Uslove i nivo podrške i održavanja tokom trajanja ugovora.	